

IN THE SUPERIOR COURT OF FULTON COUNTY  
STATE OF GEORGIA

DONNA CURLING, et al., )  
 )  
 Plaintiffs, )  
 )  
 vs. )  
 )  
 BRIAN P. KEMP, in his official )  
 capacity as Secretary of State )  
 of Georgia, et al., )  
 )  
 Defendants. )  
 \_\_\_\_\_ )

CASE NO.: 2017CV290630

Exhibits to the Motion Hearing  
before the Honorable Kimberly M. Esmond Adams  
held on June 7, 2017  
at the Justice Center Tower, Courtroom 4-E

APPEARANCES OF COUNSEL:

For the Plaintiffs: EDWARD KRUGMAN  
ROBERT McGUIRE  
Attorneys at Law

For the Defendants: JOSIAH HEIDT  
CRISTINA CORREIA  
KAYE WOODARD BURWELL  
BENNETT D. BRYAN  
DANIEL WHITE  
Attorneys at Law

Kristina Weaver, RPR, CCR-B-1785

185 Central Avenue, S.W.  
Suite T-1858  
Atlanta, Georgia 30303  
(404) 612-4607

## I-N-D-E-X T-O E-X-H-I-B-I-T-S

For the Plaintiffs:

<u>EXHIBIT</u>	<u>TENDERED</u>	<u>ADMITTED</u>
2 Email/KSU Report	167	167
6 Felten Affidavit	27	28
10 Certifications	136	136
14 Form 990	157	157
16 Open Records Request Exchanges	162	162
18 Three Member Names of RMF	117	118
26 Data Flow Chart	34	34
27 Components Chart	163	164

For the Defendants:

<u>EXHIBIT</u>	<u>TENDERED</u>	<u>ADMITTED</u>
1 Articles of Incorporation	150	151
2 Advance Voting Numbers	223	224

Zimbra

darmstea@kennesaw.edu

---

**Re: Incident Reponse Walk through**

---

**From :** Stephen C. Gay <sgay@kennesaw.edu>

Mon, Apr 24, 2017 12:01 PM

**Subject :** Re: Incident Reponse Walk through

1 attachment

**To :** Merle King <mking@kennesaw.edu>, Michael Barnes  
<mbarne28@kennesaw.edu>

**Cc :** Lectra Lawhorne <llawhorn@kennesaw.edu>, Christopher M.  
Dehner <cmd9090@kennesaw.edu>

Merle & Michael,

Following up on this, one of the areas in which we are actively looking to grow is in the "Post-Incident Activity" area and specifically working to understand what vectors led to a compromise and what KSU could have done better to close those vectors (or minimally detected earlier). For the Center for Election Systems incident, we adopted a format which GaTech shared to conduct document incident "After Action Reports". The document purposely vague in regards to the incident, but is highly tactical in prescribing mitigation steps to prevent future incidents.

Can I ask you to review and provide your feedback, as I value your input and all mitigation is going to be conducted in a secure and collaborative manner.

Thank you,  
Stephen

----- Original Message -----

From: "Merle King" <mking@kennesaw.edu>  
To: "Stephen C Gay" <sgay@kennesaw.edu>  
Cc: "Michael Barnes" <mbarne28@kennesaw.edu>, "Lectra Lawhorne" <llawhorn@kennesaw.edu>, "Steven Dean" <sdean29@kennesaw.edu>  
Sent: Tuesday, April 18, 2017 9:55:05 AM  
Subject: Incident Reponse Walk through

Stephen - We are looking for assistance in designing and conducting an incident response exercise walk through for several difference scenarios here at the Center. Do you have a template or other guidelines that can help us organize the exercise? We would like to include our staff, UITS, and SOS IT staff in the exercise.

Thanks in advance,

Merle

--

Merle S. King

Executive Director  
Center for Election Systems  
Kennesaw State University  
3205 Campus Loop Road  
Kennesaw, Georgia 30144



Voice: 470-578-6900

Fax: 470-578-9012

---

— **CES AAR.docx**

45 KB

---



Center for Election Systems  
Incident Date: March 1, 2017

## Background

On Wednesday March 1<sup>st</sup> at 9:29pm, a member of the KSU UITS Information Security Office was contacted by a KSU faculty member regarding an alleged breach of data on the elections.kennesaw.edu server. UITS staff validated the vulnerability and notified the CIO regarding the incident. The data contained hosted on the identified server was outside the scope of student information and no student records are associated with this alleged breach. Log analysis identified that the largest file identified contained voter registration information for 6.7 million individuals.

## Actions Taken

Within an hour of initial contact, the vulnerability was confirmed and firewall rules established to block access to elections.kennesaw.edu. On March 2, 2017, UITS-ISO pulled apache and Drupal logs, reported incident to USG, reset passwords, and seized the elections.kennesaw.edu server. On March 3, 2017, the FBI was engaged and the impacted server was turned over to FBI for investigation.

IT staff which were reporting within the Center for Election systems were realigned to report within the University Information Technology Services Information Security Office and a walkthrough of the area performed to validate the isolated internal network's segregation from the public network. The elections backup server – unicoi – was removed from the Center and physically secured within UITS ISO Evidence Storage.

On March 30<sup>th</sup>, KSU employees (President Olens, CIO, AVP Strategic Communications, Legal Counsel, CISO, CES Representatives) met with the FBI and US Attorney's Office regarding the outcome of the Federal Investigation. Chad Hunt shared that the investigation had yielded no data that "escalates to the point of breach". KSU Released a statement to the media on 3/31/17 as follows:

**KENNESAW, Ga (Mar. 31, 2017)** –Kennesaw State officials report there is no indication of any illegal activity and that no personal information was compromised following unauthorized access of a dedicated server at the Center for Election Systems. KSU officials were briefed yesterday by the Federal Bureau of Investigation (FBI).

University officials were first notified of the situation on March 1 and immediately isolated the server. Officials also contacted the Office of the Secretary of State and federal law enforcement, which prompted the FBI investigation. According to the FBI, the server was accessed by an outside security researcher. No student data was involved.

"We are working with experts within the University System of Georgia and an outside firm to validate that KSU's systems are secured and meet best practice standards," said KSU President Sam Olens. "We greatly appreciate the speed and dedication of the FBI and the U.S. Attorney's Office in helping us resolve this issue."



## Center for Election Systems

Incident Date: March 1, 2017

None, although if it was determined that the data hosted on elections.kennesaw.edu was maliciously disclosed, the notification and credit monitoring would have been approximately \$2 million.

**Successes**

The following list describes those actions or systems that worked as intended, or better than anticipated, during the execution of incident and breach response activities:

- The UITS ISO Incident Response process worked as intended, isolating the server and preserving evidence for later analysis and hand-off to federal authorities.
- The time between initial report and the server being isolated was approximately 60 minutes.
- The open dialog between the faculty incident reporter and the Office of the CIO staff facilitated timely notification and rapid response time.
- Having regular conversations with Legal Affairs, Strategic Communications, Center for Election Systems staff, and the Office of the CIO ensured that all parties were informed on developments, allowing for individual planning in each respective area.

**Opportunities for Improvement**

1. **Issue:** Poor understanding of risk posed by The Center for Election Systems IT systems. While a previous server scan and an external researcher had helped UITS understand the high threat level of CES systems, the lack of understanding the hosted data set led to an incomplete picture of the asset value. This resulted in the existence of a high risk server (High Asset Value / High Threat Level) which should have been prioritized.

**Action item(s):** An objective 3<sup>rd</sup> party was hired to conduct a threat assessment for externally-facing applications. In addition, funding was secured to extend the current KSU vulnerability scanning engine to allow for external scans. Once these scans are complete, a thorough analysis of all vulnerable systems will quantify the threat level and remediation plans will be developed (and incorporated into remediation projects)

**Action Item Owner(s):** UITS Information Security Office

2. **Issue:** Elections webserver and Unicoi backup server are running a vulnerable version of Drupal and vulnerable to exploitation.

**Action Items:** Elections (externally-facing) was seized immediately and Unicoi (isolated network) was seized thereafter. Both were placed in ISO Secure Storage. UITS provisioned a dedicated virtual server, FS-ES, and business documents were moved to a newly provisioned server. This share is limited the CES subnet and CES Active Directory group users. Server administrators are limited to 2 UITS ISS Staff Members.

**Action Item Owner:** UITS-ISO, UITS-ISS, CES Staff

3. **Issue:** CES confidential data handling processes were not defined.

**Action Items:** Business processes were developed, documented, and implemented to ensure confidential data is handled appropriately. CES technicians were issued IronKey encrypted hard



UITS Information Security Office

Center for Election Systems

Incident Date: March 1, 2017

drives and secure FTP transfers established with Georgia Secretary of State's Office. To date, all processes have been approved by the Georgia Secretary of State's Office.

**Action Item Owner:** UITS-ISO, CES Staff, Georgia Secretary of State Office

4. **Issue:** Center for Election System IT staff is not aligned with the University Information Technology Services, creating a scenario in which institutional risk could be accepted without CIO awareness.

**Action Items:** CES IT staff reporting structure realigned to mirror UITS TSS model. CES IT staff will report directly to UITS-ISO while directly supporting the CES. Additionally, all processes will align with USG and KSU data security policies. Strategically, UITS is launching a project to engage all external IT in order to better understand university-wide IT risk.

**Action Item Owner:** UITS-ISO, CES Staff

5. **Issue:** Room 105a, the elections private network data closet, was not latching properly due to lock/door misalignment.

**Action Items:** CISO contacted Chief of Police to have lock and door aligned. Work was completed within one business day. ISO to develop processes to review access logs on a scheduled basis.

**Action Item Owner:** UITS-ISO, KSU UPD, CES Staff

6. **Issue:** The elections private network data closet contains a live network jack to the ~~public network~~ (Public network)

**Action Items:** UITS-ISO should acquire color-coded Ethernet Jack block-outs to "lock" all ports in the data closet to the public network AND to "lock" all ports to the private network outside the data closet. Key's should be maintained by ISS and ISO, necessitating consulting with UITS staff before connecting devices.

**Action Item Owner:** UITS-ISO, UITS-ISS

7. **Issue:** A number of IT Assets within the Center for Elections Systems have reached end-of-life and need to be replaced or migrated to different infrastructure.

1. Rackmount UPS Battery backups (one displaying warning light)

Recommendation: Replace batteries as needed and move under UITS ISS management

2. 3com Switches – Age 10+ years -- No Support -- L2 only

Recommendation: Replace and move under UITS ISS management

3. Dell 1950 (Windows Domain Controller) – Age 10+ years

Recommendation: Surplus

4. Dell PowerEdge R630 – Age 1 year

Recommendation: Migrate services from Dell 1950 and move under UITS ISS management on CES Isolated Network

5. EPIC – Vision Computer – Age Unknown – Ballot creation box

Recommendation: Continue as ISO/CES managed

6. EPIC Files – Dell 1900 – Age 6+ years – Ballot backups

Recommendation: Surplus

7. NAS – Dell 1900 – Age 6+ years – CES Isolated Network NAS

Recommendation: Surplus

8. elections.kennesaw.edu - Age 5 years - Dell PowerEdge R610



UITS Information Security Office

Center for Election Systems

Incident Date: March 1, 2017

Recommendation: Format and reinstall on CES Isolated Network as NAS

9. unicoi.kennesaw.edu – Age 6+ years. Dell PowerEdge 1950

Recommendation: Surplus

10. Web server backup

Recommendation: Surplus

**Action Item Owner:** UITS-ISO, UITS-ISS, CES Staff

**8. Issue:** An operating system and application security assessment has not been conducted on the CES Isolated Network

**Action Items:** UITS-ISO should perform a stand-alone security assessment of the CES Isolated Network using a laptop-based scanning engine. Servers and workstations should be hardened based on the scan results and regular testing of the network scheduled.

**Action Item Owner:** UITS-ISO, UITS-ISS, CES Staff

**9. Issue:** A wireless access point was found when UITS did a walkthrough of the CES House

**Action Items:** Understanding the risk that a wireless access point presents to the CES isolated network, UITS-ISO should prioritize CES for wireless network upgrade and put guidelines in place which prohibit the use of non-KSU wireless devices in the house.

**Action Item Owner:** UITS-ISO, UITS-ISS

**10. Issue:** Inconsistent port colors in House 57. Data outlets throughout the building have different color bezels to indicate which network is public and which is private:

Red = analog voice/phone

Green = KSU data public network

Blue = Elections private network

White = Elections 2nd private network

Since the original cabling installation the two private networks established for elections now act as a single private network. In room 105a, the blue cables terminate to one patch panel and the white cables terminate to another patch panel. They have connected jumpers from both of these patch panels to the same switch thus eliminating any separation by the colors Blue or White.

**Action Items:** Jacks for the public and private network should be reinstalled to conform to campus color standards. Additionally, jacks from the public and private networks should be on different panels. The total cost of this change will be approximately \$3,000.

**Action Item Owner:** UITS-ISO, UITS-ISS

**IN THE SUPERIOR COURT OF FULTON COUNTY  
STATE OF GEORGIA**

DONNA CURLING, an individual; )  
 )  
 DONNA PRICE, an individual; )  
 )  
 ROCKY MOUNTAIN FOUNDATION, )  
 INC., a non-profit corporation organized )  
 and existing under Colorado law; )  
 )  
 Plaintiffs, )  
 )  
 v. )  
 )  
 BRIAN P. KEMP, in his official capacity )  
 as Secretary of State of Georgia; )  
 )  
 RICHARD BARRON, in his official )  
 capacity as Director of the Fulton County )  
 Board of Elections and Registration; )  
 )  
 MAXINE DANIELS, in her official )  
 capacity as Director of Voter Registrations )  
 and Elections for DeKalb County; )  
 )  
 JANINE EVELER, in her official )  
 capacity as Director of the Cobb County )  
 Board of Elections and Registration; )  
 )  
 Defendants. )

CIVIL ACTION  
FILE NO.:

**AFFIDAVIT**

County of Mercer )  
 ) ss.  
 State of New Jersey )

**EDWARD W. FELTEN** ("Affiant"), being of lawful age and first duly sworn upon oath, deposes and states as follows:

1. I am the Robert E. Kahn Professor of Computer Science and Public Affairs at Princeton University, and the Director of Princeton's Center for Information Technology Policy. I received my Ph.D. in Computer Science and Engineering from the University of Washington in 1993. I am a member of the National Academy of Engineering and the American Academy of Arts and Sciences.

Plaintiff's Exhibit

6

06/07/2017 Hearing

2. From 2015 until January 2017, I served in the White House as Deputy United States Chief Technology Officer. During that time I advised the President and his senior advisors on policy issues relating to computer science, including issues relating to the security and reliability of elections and electronic voting systems.

3. A copy of my curriculum vitae is attached as Exhibit A.

**Inherent risks of paperless electronic voting machines**

4. Before turning to the specific systems and circumstances of this matter, I will provide a brief summary of cybersecurity issues relating to voting machines.

5. The voting machines at issue in this matter are a type of so-called Direct Recording Electronic (DRE) machine. DREs are voting machines that are designed to record a voter's ballot directly in electronic storage, without creating any record of the ballot that can be directly verified by the voter.

6. DREs can be contrasted with other voting technologies in which there is a record of the voter's ballot, typically on paper, the accuracy of which can be verified directly by the voter in the polling place, and which is collected at the polling place as a record of the voter's intent. The most common examples of voter-verifiable ballots include paper ballots. The simplest way to tabulate paper ballots is by hand counting.

7. The lack of a voter-verifiable ballot creates special risks associated with any DRE voting system. For this reason, computer scientists and cybersecurity experts typically recommend against the use of DREs. I concur with this general recommendation against the use of DREs.

8. The hardware of a DRE—the physical equipment comprising the computer—is much like a standard desktop computer, often installed into a different physical enclosure. Like a standard computer, a DRE will do whatever the software installed in it directs it to do. If anyone changes the software, whether through malice or error, the DRE may do something other than accurately recording and tabulating votes.

9. A malicious modification to a DRE's software would likely cause the DRE to modify ballots silently. The modified software could be designed to report on the machine's display screen, to voters and election officials, that all was well. It could also be designed to falsify all of the logs and records kept by the voting machine.

10. My students and I have modified the software on many types of DREs. For example, my students modified a (now decommissioned) New York DRE to turn it into a kiosk for playing the popular arcade game Pac-Man. We have also created, installed, and tested software for multiple DRE models that would silently modify election results. (For obvious reasons, these latter tests were done in secure laboratories.)

**My team's study of Diebold voting machines**

11. I led a team of researchers that studied the Diebold AccuVote TS voting machine system. We published a peer-reviewed paper summarizing our analysis, which is attached as Exhibit B.

12. As part of our research we demonstrated that it was possible to create a voting machine virus: a computer virus that infected the voting machines, spreading from machine to machine by infecting the memory cards that are used to transport election and ballot information between the machines and central tabulation offices. The virus, having infected a voting machine, would modify election results, without leaving any trace in the logs or records kept by the machine. We created and tested such a virus in our secure laboratory.

13. I did a live demonstration of this election-stealing virus, including showing the casting of votes and mis-reporting of the vote counts by the machine, during live testimony at a hearing of a committee of the U.S. House of Representatives. My students and I did a similar demonstration twice on live television, on CNN and Fox News.

14. The TS machine we studied allowed modified (and possibly malicious) software to be installed by anyone who could open a small metal access door on the side of the machine. The door was locked by an ordinary file cabinet type of lock. Because the very same key that is used for the access door on the AccuVote TS is also used widely on office furniture, jukeboxes, and hotel minibars, the keys are easily purchased. I bought a gross of these keys (i.e., 144 keys) from a vendor on the Internet. The lock is also easily picked—a member of our team who studies locks as hobby was able to pick the access door lock consistently in less than 15 seconds.

15. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes.

16. Our peer reviewed paper listed a number of other security problems with the AccuVote TS system. Some of these problems could in principle be fixable by improving the software of the TS, but others are inherent in the machine's hardware and therefore not fixable by any software update.

17. As described in our peer reviewed paper, it is inherent in the hardware design of the TS that a person who can get physical access to the inside of the machine can install any software they like on the machine.

18. In short, we demonstrated that a person with access to a TS machine can modify its software, and that this modification can render the machine unable to accurately record or tabulate votes. This problem is inherent in the hardware design of the TS machine.

19. Subsequent to the publication of our paper, we studied the AccuVote TSX system and found that it had similar security problems.

#### **Need for software verification**

20. One cannot know that any DRE machine, including a TS or TSX, will accurately record or tabulate votes, unless one is certain as to which software is installed on that machine. Because of the ease of malicious modification of the software, it is not enough to know which software is supposed to be installed—one must inspect the machine to verify which software is actually installed.

21. Verifying which software is actually installed is technically very difficult, because one cannot rely on the software itself to report its own status accurately. Malicious software can simply misreport its own status, reporting that everything is normal. Relying on the software to report whether it has been tampered with is like trying to determine whether a person is honest by asking him, “Are you honest?” An answer of “yes” is not reliable evidence.

22. Unfortunately, the standard methods for inspecting the software version installed in a machine rely on the machine’s software in one way or another, so they fail to avoid this pitfall and should not be trusted. Special protocols, typically involving the use of specialized equipment, must be designed and used to perform such inspections, and rigorous chain-of-custody controls are necessary after the inspection to make sure no tampering with the machine’s software could have occurred after the inspection.

23. Unless all of these steps are followed, with respect to a particular DRE machine, one cannot be confident in its ability to accurately record or tabulate votes.

#### **Need for secure facilities**

24. I understand that Georgia voting machines are tested and configured in the Center for Election Systems (CES) at Kennesaw State University (KSU). Because my team’s research has demonstrated the propagation of malicious software during these types of activities, any security breach at CES, or failure to implement adequate cybersecurity precautions at CES, could have created an opportunity for a malicious party to modify software in voting machines and related systems.

25. The security breach at CES, and KSU’s response to it, are indications that cybersecurity precautions at CES may not have been adequate. It is especially significant that KSU’s response to the breach included steps to change how cybersecurity and system administration were managed at CES, so that CES personnel were no longer managing these functions on their own.

26. The most sophisticated cyberattackers are especially skilled not only at gaining unauthorized access to systems, but also at maintaining access. So-called Advanced Persistent Threat actors specialize in gaining access and maintaining that access over time, while avoiding detection and waiting for the best moment to strike. Once they are in a system, it can be

extraordinarily difficult to find them. As a result, very stringent measures may be necessary to render a facility safe after a period of vulnerability—and especially when highly skilled actors may have been motivated to compromise that facility.

27. Because of the vulnerability of the DRE voting machines to software manipulation, and because of intelligence reports about highly skilled cyber-actors having attempted to affect elections in the United States, such precautions appear to be indicated for the CES systems. In the absence of stringent precautions to find and expel potential intruders in the CES systems, the ability of voting-related systems that have been in the CES facility to function correctly and securely should be viewed with greater skepticism.

28. Further Affiant sayeth not.

 May 26, 2017  
Edward W. Felten

  
**EMMA MARSHALL**  
**NOTARY PUBLIC OF NEW JERSEY**  
**I.D. # 2434585**  
**My Commission Expires 5/30/2018**

## **Edward W. Felten**

### **Education**

Ph.D. in Computer Science and Engineering, University of Washington, 1993.

Dissertation title: "Protocol Compilation: High-Performance Communication for Parallel Programs." Advisors: Edward D. Lazowska and John Zahorjan.

M.S. in Computer Science and Engineering, University of Washington, 1991.

B.S. in Physics, with Honors, California Institute of Technology, 1985.

### **Employment**

Robert E. Kahn Professor of Computer Science and Public Affairs, Princeton University, 2013-present

Deputy United States Chief Technology Officer, The White House, Office of Science and Technology Policy, 2015-2017

Professor of Computer Science and Public Affairs, Princeton University, 2006-2013.

Chief Technologist, U.S. Federal Trade Commission, 2011-2012.

Professor of Computer Science, Princeton University, 2003-2006.

Associate Professor of Computer Science, Princeton University, 1999-2003.

Assistant Professor of Computer Science, Princeton University, 1993-99.

Senior Computing Analyst, Caltech Concurrent Computing Project, California Institute of Technology, 1986-1989.

Director, Center for Information Technology Policy, Princeton University, 2005-present.

Elysium Digital LLC and various law firms. Consulting and expert testimony in technology litigation, 1998-2015

U.S. Federal Trade Commission: consulting regarding spam policy and investigation, 2004, 2006.

U.S. Dept. of Justice, Antitrust Division: consulting and testimony in Microsoft antitrust case, 1998-2002..

Electronic Frontier Foundation. Consulting in intellectual property / free speech lawsuits, 2001-2010.

Certus Ltd.: consultant in product design and analysis, 2000-2002.

Cigital Inc.: Technical Advisory Board member, 2000-2007.

Cloakware Ltd.: Technical Advisory Board member, 2000-2003.

Propel.com: Technical Advisory Board member, 2000-2002.

NetCertainty.com: Technical Advisory Board member, 1999-2002.  
FullComm LLC: Scientific Advisory Board member, 1999-2001.  
Sun Microsystems: Java Security Advisory Board member, 1997-2001.  
Finjan Software: Technical Advisory Board member, 1997-2002.  
International Creative Technologies: consultant in product design and analysis, 1997-98.  
Bell Communications Research: consultant in computer security research, 1996-97.

## **Honors and Awards**

National Academy of Engineering, 2013.  
Alumni Achievement Award, University of Washington, 2013.  
American Academy of Arts and Sciences, 2011.  
E-Council Teaching Award, School of Engineering and Appl. Sci., Princeton, 2010.  
ACM Fellow, 2007.  
EFF Pioneer Award, 2005.  
Scientific American Fifty Award, 2003.  
Alfred P. Sloan Fellowship, 1997.  
Emerson Electric, E. Lawrence Keyes Faculty Advancement Award, Princeton University School of Engineering, 1996.  
NSF National Young Investigator award, 1994.  
Outstanding Paper award, 1997 Symposium on Operating Systems Principles.  
Best Paper award, 1995 ACM SIGMETRICS Conference.  
AT&T Ph.D. Fellowship, 1991-93.  
Mercury Seven Foundation Fellowship, 1991-93.

## **Research Interests**

Information security. Privacy. Technology law and policy. Internet software.  
Intellectual property policy. Using technology to improve government. Operating systems. Distributed computing. Parallel computing architecture and software.

## **Professional Service**

### ***Professional Societies and Advisory Groups***

ACM U.S. Public Policy Council, Chair, 2014-2015.  
ACM U.S. Public Policy Committee, Vice Chair, 2008-2010, 2012-2014.  
DARPA Privacy Panel, 2010-2012.  
Transportation Security Administration, Secure Flight Privacy Working Group, 2005.  
National Academies study committee on Air Force Information Science and Technology Research, 2004.  
Electronic Frontier Foundation, Advisory Board, 2004-2007.  
ACM U.S. Public Policy Committee, 2004-present (Executive Committee, 2005-present)

ACM Advisory Committee on Security and Privacy, 2002-2003.  
DARPA Information Science and Technology (ISAT) study group, 2002-2004.  
Co-chair, ISAT study committee on "Reconciling Security with Privacy," 2001-2002.  
National Academy study committee on Foundations of Computer Science, 2001-2004.

### ***Program Committees***

World Wide Web Conference, 2006.  
USENIX General Conference, 2004.  
Workshop on Foundations of Computer Security, 2003.  
ACM Workshop on Digital Rights Management, 2001.  
ACM Conference on Computer and Communications Security, 2001.  
ACM Conference on Electronic Commerce, 2001.  
Workshop on Security and Privacy in Digital Rights Management, 2001.  
Internet Society Symposium on Network and Distributed System Security, 2001.  
IEEE Symposium on Security and Privacy, 2000.  
USENIX Technical Conference, 2000.  
USENIX Windows Systems Conference, 2000.  
Internet Society Symposium on Network and Distributed System Security, 2000.  
IEEE Symposium on Security and Privacy, 1998.  
ACM Conference on Computer and Communications Security, 1998.  
USENIX Security Symposium, 1998.  
USENIX Technical Conference, 1998.  
Symposium on Operating Systems Design and Implementation, 1996.

### ***Boards***

Verified Voting, Advisory Board, 2013-present.  
Electronic Privacy Information Center, Advisory Board, 2013-present.  
Electronic Frontier Foundation, Board of Directors, 2007-2010.  
DARPA Information Science and Technology study board, 2001-2003.  
Cigital Inc.: Technical Advisory Board (past).  
Sun Microsystems, Java Security Advisory Council (past).  
Cloakware Ltd.: Technical Advisory Board (past).  
Propel.com: Technical Advisory Board (past).  
Finjan Software: Technical Advisory Board (past).  
Netcertainty: Technical Advisory Board (past).  
FullComm LLC: Scientific Advisory Board (past).

### ***University and Departmental Service***

Council on Teaching and Learning, 2014-2015.  
School of Engineering and Appl. Sci., Strategic Plan Steering Committee, 2014-2015  
Committee on Online Courses, 2012-2013.  
Director, Center for Information Technology Policy, 2005-present.  
Committee on the Course of Study, 2009-present.  
SEAS Strategic Planning, 2004.  
    Member, Executive Committee  
    Co-Chair, Interactions with Industry area.

Co-Chair, Engineering, Policy, and Society area.  
Faculty Advisory Committee on Policy, 2002-present.  
Council of the Princeton University Community, 2002-present (Executive Committee)  
Faculty Advisory Committee on Athletics, 1998-2000.  
Computer Science Academic Advisor, B.S.E. program, class of 1998 (approx. 25 students)  
Faculty-Student Committee on Discipline, 1996-98.  
Faculty-Student Committee on Discipline, Subcommittee on Sexual Assault and Harrassment, 1996-98.

## **Students Advised**

### ***Ph.D. Advisees:***

Harlan Yu (Ph.D. 2012). Dissertation: Designing Software to Shape Open Government Policy. Founder, Upturn Partners.  
Ariel J. Feldman (Ph.D. 2012). Dissertation: Privacy and Integrity in the Untrusted Cloud. Assistant Professor of Computer Science, University of Chicago.  
Joseph A. Calandrino (Ph.D. 2012). Dissertation: Control of Sensitive Data in Systems with Novel Functionality. Consulting Computer Scientist, Elysium Digital.  
William B. Clarkson (Ph.D. 2012). Dissertation: Breaking Assumptions: Distinguishing Between Seemingly Identical Items Using Cheap Sensors. Technical staff member at Google.  
Matthias Jacob (Ph.D. 2009). Technical staff member at Nokia.  
J. Alex Halderman (Ph.D. 2009). Dissertation: Security Failures in Non-traditional Computing Environments. Associate Professor of Computer Science, University of Michigan.  
Shirley Gaw (Ph.D. 2009). Dissertation: Ideals and Reality: Adopting Secure Technologies and Developing Secure Habits to Prevent Message Disclosure. Technical staff member at Google.  
Brent Waters (Ph.D. 2004). Dissertation: Security in a World of Ubiquitous Recording Devices. Professor of Computer Science, University of Texas.  
Robert A. Shillingsburg (Ph.D. 2004). Dissertation: Improving Distributed File Systems using a Shared Logical Disk. Retired; previously a technical staff member at Google.  
Michael Schneider (Ph.D. 2004). Dissertation: Network Defenses against Denial of Service Attacks. Researcher, Supercomputing Research Center, Institute for Defense Analyses.  
Minwen Ji (Ph.D. 2001). Dissertation: Data Distribution for Dynamic Web Content. Researcher, HP Labs.  
Dirk Balfanz (Ph.D. 2000). Dissertation: Access Control for Ad Hoc Collaboration. Technical staff member at Google.  
Dan S. Wallach (Ph.D. 1998). Dissertation: A New Approach to Mobile Code Security. Professor of Computer Science, Rice University.

***Significant Advisory Role:***

Drew Dean (Ph.D. 1998). Advisor: Andrew Appel. Research Scientist, SRI International.

Stefanos Damianakis (Ph.D. 1998). Advisor: Kai Li. President and CEO, Netrics, Inc.

Pei Cao (Ph.D. 1996). Advisor: Kai Li. Technical staff at Facebook.

Lujo Bauer (Ph.D. 2003). Advisor: Andrew Appel. Associate Professor, School of Computer Science, Carnegie Mellon University.

## **Publications**

### ***Books and Book Chapters***

- [1] The Economics of Bitcoin, or Bitcoin in the Presence of Adversaries. Joshua A. Kroll, Ian Davey, and Edward W. Felten. To appear, Lecture Notes in Computer Science series.
- [2] Enabling Innovation for Civic Engagement. David G. Robinson, Harlan Yu, and Edward W. Felten. In *Open Government*, Daniel Lathrop and Laurel Ruma, eds., O'Reilly, 2010.
- [3] *Securing Java: Getting Down to Business with Mobile Code*. Gary McGraw and Edward W. Felten. John Wiley and Sons, New York 1999.
- [4] *Java Security: Web Browsers and Beyond*. Drew Dean, Edward W. Felten, Dan S. Wallach, and Dirk Balfanz. In "Internet Besieged: Countering Cyberspace Scofflaws," Dorothy E. Denning and Peter J. Denning, eds. ACM Press, New York, 1997.
- [5] *Java Security: Hostile Applets, Holes and Antidotes*. Gary McGraw and Edward Felten. John Wiley and Sons, New York, 1996
- [6] *Dynamic Tree Searching*. Steve W. Otto and Edward W. Felten. In "High Performance Computing", Gary W. Sabot, ed., Addison Wesley, 1995.

### ***Journal Articles***

- [7] Accountable Algorithms. Joshua A. Kroll, Joanna Huey, Solon Barocas, Edward W. Felten, Joel R. Reidenberg, David G. Robinson, and Harlan Yu. *University of Pennsylvania Law Review*, Vol. 165, 2017. *Forthcoming. 2016 Future of Privacy Forum Privacy Papers for Policymakers Award*.
- [8] Government Data and the Invisible Hand. David Robinson, Harlan Yu, William Zeller, and Edward W. Felten. *Yale Journal of Law and Technology*, vol. 11, 2009.
- [9] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. *Software – Practice and Experience*, 33:461-480, 2003.
- [10] The Digital Millennium Copyright Act and its Legacy: A View from the Trenches. *Illinois Journal of Law, Technology and Policy*, Fall 2002.
- [11] The Security Architecture Formerly Known as Stack Inspection: A Security Mechanism for Language-based Systems. Dan S. Wallach, Edward W. Felten, and Andrew W. Appel. *ACM Transactions on Software Engineering and Methodology*, 9:4, October 2000.

- [12] Statically Scanning Java Code: Finding Security Vulnerabilities. John Viega, Tom Mutdosch, Gary McGraw, and Edward W. Felten. IEEE Software, 17(5), Sept./Oct. 2000.
- [13] Client-Server Computing on the SHRIMP Multicomputer. Stefanos N. Damianakis, Angelos Bilas, Cezary Dubnicki, and Edward W. Felten. IEEE Micro 17(1):8-18, February 1997.
- [14] Fast RPC on the SHRIMP Virtual Memory Mapped Network Interface. Angelos Bilas and Edward W. Felten. IEEE Transactions on Parallel and Distributed Computing, February 1997.
- [15] Implementation and Performance of Integrated Application-Controlled File Caching, Prefetching and Disk Scheduling. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. ACM Transactions on Computer Systems, Nov 1996.
- [16] Virtual Memory Mapped Network Interface Designs. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, Kai Li, and Malena Mesarina. IEEE Micro, 15(1):21-28, February 1995.

***Selected Symposium Articles***

- [17] Research Perspectives and Challenges for Bitcoin and Cryptocurrencies. Joseph Bonneau, Andrew Miller, Jeremy Clark, Arvind Narayanan, Joshua A. Kroll, and Edward W. Felten. IEEE Symposium on Security and Privacy, 2015.
- [18] A Precautionary Approach to Big Data Privacy. Edward W. Felten, Joanna Huey, and Arvind Narayanan. Conference on Privacy and Data Protection, 2015.
- [19] On Decentralizing Prediction Markets and Order Books. Jeremy Clark, Joseph Bonneau, Edward W. Felten, Joshua A. Kroll, Andrew Mill, and Arvind Narayanan. Workshop on Economics of Information Security, May 2014.
- [20] Mixcoin: Anonymity for Bitcoin with Accountable Mixes. Joseph Bonneau, Arvind Narayanan, Andrew Miller, Jeremy Clark, Joshua A. Kroll, and Edward W. Felten. Proceedings of Financial Cryptography, February 2014.
- [21] Privacy Concerns of Implicit Security Factors for Web Authentication. Joseph Bonneau, Edward W. Felten, Prateek Mittal, and Arvind Narayanan. Adventures in Authentication: WAY Workshop, 2014.
- [22] The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries. Joshua Kroll, Ian Davey, and Edward W. Felten. Workshop on the Economics of Information Security, 2013.
- [23] Social Networking with Frientegrity: Privacy and Integrity with an Untrusted Provider. Ariel J. Feldman, Aaron Blankstein, Michael J. Freedman, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2012.
- [24] Bubble Trouble: Off-Line De-Anonymization of Bubble Forms. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. USENIX Security Symposium, Aug. 2011.

- [25] You Might Also Like: Privacy Risks of Collaborative Filtering. Joseph A. Calandrino, Ann Kilzer, Arvind Narayanan, Edward W. Felten, and Vitaly Shmatikov. Proc. IEEE Symposium on Security and Privacy, May 2011.
- [26] SPORC: Group Collaboration Using Untrusted Cloud Resources. Ariel J. Feldman, William P. Zeller, Michael J. Freedman, and Edward W. Felten. Proc. Symposium on Operating Systems Design and Implementation, 2010.
- [27] SVC: Selector-Based View Composition for Web Frameworks. William Zeller and Edward W. Felten. Proc. USENIX Conference on Web Application Development, 2010.
- [28] Defeating Vanish with Low-Cost Sybil Attacks Against Large DHTs. Scott Wolchok, Owen S. Hofmann, Nadia Heninger, Edward W. Felten, J. Alex Halderman, Christopher J. Rossbach, Brent Waters, and Emmet Witchel. Proc. 17<sup>th</sup> Network and Distributed System Security Symposium, 2010.
- [29] Can DREs Provide Long-Lasting Security? The Case of Return-Oriented Programming and the AVC Advantage. Stephen Checkoway, Ariel J. Feldman, Brian Kantor, J. Alex Halderman, Edward W. Felten, and Hovav Shacham, Proc. Electronic Voting Technology Workshop, 2009.
- [30] Some Consequences of Paper Fingerprinting for Elections. Joseph A. Calandrino, William Clarkson, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2009.
- [31] Software Support for Software-Independent Auditing. Gabrielle A. Gianelli, Jennifer D. King, Edward W. Felten, and William P. Zeller. Proc. Electronic Voting Technology Workshop, 2009.
- [32] Fingerprinting Blank Paper Using Commodity Scanners. William Clarkson, Tim Weyrich, Adam Finkelstein, Nadia Heninger, J. Alex Halderman, and Edward W. Felten. Proc. ACM Symposium on Security and Privacy, May 2009.
- [33] Lest We Remember: Cold Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. Proc. Usenix Security Symposium, 2008.
- [34] In Defense of Pseudorandom Sample Selection. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2008.
- [35] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.
- [36] Machine-Assisted Election Auditing. Joseph A. Calandrino, J. Alex Halderman, and Edward W. Felten. Proc. Electronic Voting Technology Workshop, 2007.
- [37] Lessons from the Sony CD DRM Episode. J. Alex Halderman and Edward W. Felten. Proc. Usenix Security Symposium, 2006.

- [38] A Convenient Method for Securely Managing Passwords. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. Proc. 14<sup>th</sup> World Wide Web Conference, 2005.
- [39] New Client Puzzle Outsourcing Techniques for DoS Resistance. Brent R. Waters, Ari Juels, J. Alex Halderman, and Edward W. Felten. ACM Conference on Computer and Communications Security. November 2004.
- [40] Privacy Management for Portable Recording Devices. J. Alex Halderman, Brent R. Waters, and Edward W. Felten. 3<sup>rd</sup> Workshop on Privacy in Electronic Society. November 2004.
- [41] Receiver Anonymity via Incomparable Public Keys. Brent R. Waters, Edward W. Felten, and Amit Sahai. ACM Conference on Computer and Communications Security. November 2003.
- [42] Attacking an Obfuscated Cipher by Injecting Faults. Matthias Jacob, Dan Boneh, and Edward W. Felten. ACM Workshop on Digital Rights Management, November 2002.
- [43] A General and Flexible Access-Control System for the Web. Lujo Bauer, Michael A. Schneider, and Edward W. Felten. 11<sup>th</sup> USENIX Security Symposium, August 2002.
- [44] Informed Consent in the Mozilla Browser: Implementing Value-Sensitive Design. Batya Friedman, Daniel C. Howe, and Edward W. Felten. Hawaii International Conference on System Sciences, January 2002. (Best Paper award, organizational systems track.)
- [45] Reading Between the Lines: Lessons from the SDMI Challenge. Scott A. Craver, John P. McGregor, Min Wu, Bede Liu, Adam Stubblefield, Ben Swartzlander, Dan S. Wallach, Drew Dean, and Edward W. Felten. USENIX Security Symposium, August 2001.
- [46] Cookies and Web Browser Design: Toward Realizing Informed Consent Online. Lynette I. Millett, Batya Friedman, and Edward W. Felten. Proc. of CHI 2001 Conference on Human Factors in Computing Systems, April 2001.
- [47] Timing Attacks on Web Privacy. Edward W. Felten and Michael A. Schneider. Proc. of 7th ACM Conference on Computer and Communications Security, Nov. 2000.
- [48] Archipelago: An Island-Based File System for Highly Available and Scalable Internet Services. USENIX Windows Systems Symposium, August 2000.
- [49] Proof-Carrying Authentication. Andrew W. Appel and Edward W. Felten. Proc. of 6th ACM Conference on Computer and Communications Security, Nov. 1999.
- [50] An Empirical Study of the SHRIMP System. Matthias A. Blumrich, Richard D. Alpert, Yuqun Chen, Douglas W. Clark, Stefanos, N. Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, Margaret Martonosi, Robert A. Shillner, and Kai Li. Proc. of 25th International Symposium on Computer Architecture, June 1998.
- [51] Performance Measurements for Multithreaded Programs. Minwen Ji, Edward W. Felten, and Kai Li. Proc. of 1998 SIGMETRICS Conference, June 1998.

- [52] Understanding Java Stack Inspection. Dan S. Wallach and Edward W. Felten. Proc. of 1998 IEEE Symposium on Security and Privacy, May 1998.
- [53] Extensible Security Architectures for Java. Dan S. Wallach, Dirk Balfanz, Drew Dean, and Edward W. Felten. Proc. of 16th ACM Symposium on Operating Systems Principles, Oct. 1997. Outstanding Paper Award.
- [54] Web Spoofing: An Internet Con Game. Edward W. Felten, Dirk Balfanz, Drew Dean, and Dan S. Wallach. Proc. of 20<sup>th</sup> National Information Systems Security Conference, Oct. 1997.
- [55] Reducing Waiting Costs in User-Level Communication. Stefanos N. Damianakis, Yuqun Chen, and Edward W. Felten. Proc. of 11th Intl. Parallel Processing Symposium, April 1997.
- [56] Stream Sockets on SHRIMP. Stefanos N. Damianakis, Cezary Dubnicki, and Edward W. Felten. Proc. of 1st Intl. Workshop on Communication and Architectural Support for Network-Based Parallel Computing, February 1997. (Proceedings available as Lecture Notes in Computer Science #1199.)
- [57] Early Experience with Message-Passing on the SHRIMP Multicomputer. Richard D. Alpert, Angelos Bilas, Matthias A. Blumrich, Douglas W. Clark, Stefanos Damianakis, Cezary Dubnicki, Edward W. Felten, Liviu Iftode, and Kai Li. Proc. of 23rd Intl. Symposium on Computer Architecture, 1996.
- [58] A Trace-Driven Comparison of Algorithms for Parallel Prefetching and Caching. Tracy Kimbrel, Andrew Tomkins, R. Hugo Patterson, Brian N. Bershad, Pei Cao, Edward W. Felten, Garth A. Gibson, Anna R. Karlin, and Kai Li. Proc. of 1996 Symposium on Operating Systems Design and Implementation.
- [59] Java Security: From HotJava to Netscape and Beyond. Drew Dean, Edward W. Felten, and Dan S. Wallach. Proc. of 1996 IEEE Symposium on Security and Privacy.
- [60] Integrated Parallel Prefetching and Caching. Tracy Kimbrel, Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1996 SIGMETRICS Conference.
- [61] Software Support for Virtual Memory-Mapped Communication. Cezary Dubnicki, Liviu Iftode, Edward W. Felten, and Kai Li. Proc. of Intl. Parallel Processing Symposium, April 1996.
- [62] Protected, User-Level DMA for the SHRIMP Network Interface. Matthias A. Blumrich, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996
- [63] Improving Release-Consistent Shared Virtual Memory using Automatic Update. Liviu Iftode, Cezary Dubnicki, Edward W. Felten, and Kai Li. Proc. of 2nd Intl. Symposium on High-Performance Computer Architecture, Feb. 1996
- [64] Synchronization for a Multi-Port Frame Buffer on a Mesh-Connected Multicomputer. Bin Wei, Gordon Stoll, Douglas W. Clark, Edward W. Felten, and Kai Li. Parallel Rendering Symposium, Oct. 1995.

- [65] A Study of Integrated Prefetching and Caching Strategies. Pei Cao, Edward W. Felten, Anna R. Karlin, and Kai Li. Proc. of 1995 ACM SIGMETRICS Conference. Best Paper award.
- [66] Evaluating Multi-Port Frame Buffer Designs for a Mesh-Connected Multicomputer. Gordon Stoll, Bin Wei, Douglas W. Clark, Edward W. Felten, Kai Li, and Patrick Hanrahan. Proc. of 22nd Intl. Symposium on Computer Architecture.
- [67] Implementation and Performance of Application-Controlled File Caching. Pei Cao, Edward W. Felten, and Kai Li. Proc. of 1st Symposium on Operating Systems Design and Implementation, pages 165-178, November 1994.
- [68] Application-Controlled File Caching Policies. Pei Cao, Edward W. Felten, and Kai Li. Proc. of USENIX Summer 1994 Technical Conference, pages 171-182, 1994.
- [69] Virtual Memory Mapped Network Interface for the SHRIMP Multicomputer. Matthias A. Blumrich, Kai Li, Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Jonathan S. Sandberg. Proc. of Intl. Symposium on Computer Architecture, 1994.
- [70] Performance Issues in Non-Blocking Synchronization on Shared-Memory Multiprocessors. Juan Alemany and Edward W. Felten. Proceedings of Symposium on Principles of Distributed Computing, 1992.
- [71] Improving the Performance of Message-Passing Applications by Multithreading. Edward W. Felten and Dylan McNamee. Proceedings of Scalable High-Performance Computing Conference (SHPCC), 1992.
- [72] A Highly Parallel Chess Program. Edward W. Felten and Steve W. Otto. 1988 Conference on Fifth Generation Computer Systems.

### ***Selected Other Publications***

- [73] Testimony for Privacy and Civil Liberties Oversight Board hearing on “Defining Privacy”. November 2014. Written testimony submitted December 2014.
- [74] Heartbleed Shows Government Must Lead on Internet Security. Edward W. Felten and Joshua Kroll. *Scientific American*, July 2014.
- [75] How the NSA Piggy-Backs on Third-Party Trackers. Edward Felten and Jonathan Mayer. *Slate*, Dec. 13, 2013.
- [76] Testimony for Senate Judiciary Committee hearing on “Continued Oversight of the Foreign Intelligence Surveillance Act,” October 2, 2013.
- [77] The Chilling Effects of the DMCA. Edward Felten. *Slate*, March 29, 2013.
- [78] CALEA II: Risks of Wiretap Modifications to Endpoints. [20 authors]. Submitted to a White House working group.
- [79] Strangers in a Strange Land. Review of *Blown to Bits: Your Life, Liberty, and Happiness after the Digital Explosion*, by Abelson, Ledeen, and Lewis. *American Scientist*, 97:4. July/August 2009.

- [80] Lest We Remember: Cold-Boot Attacks on Encryption Keys. J. Alex Halderman, Seth D. Schoen, Nadia Heninger, William Clarkson, William Paul, Joseph A. Calandrino, Ariel J. Feldman, Jacob Appelbaum, and Edward W. Felten. *Communications of the ACM*, 52(5):91-98. May 2009.
- [81] Security Analysis of the Diebold AccuVote-TS Voting Machine. Ariel J. Feldman, J. Alex Halderman, and Edward W. Felten. Sept. 2006.
- [82] Digital Rights Management, Spyware, and Security. Edward W. Felten and J. Alex Halderman, *IEEE Security and Privacy*, Jan./Feb. 2006.
- [83] Inside RISKS: DRM and Public Policy. Edward W. Felten. *Communications of the ACM*, 48:7, July 2005.
- [84] Understanding Trusted Computing: Will its Benefits Outweigh its Drawbacks? Edward W. Felten. *IEEE Security and Privacy*, May 2003.
- [85] A Skeptical View of DRM and Fair Use. Edward W. Felten. *Communications of the ACM* 46(4):56-61, April 2003.
- [86] Consumer Privacy and Government Technology Mandates in the Digital Media Marketplace. Testimony before U.S. Senate Commerce Committee. September 2003.
- [87] Secure, Private Proofs of Location. Brent R. Waters and Edward W. Felten. Submitted for publication, 2003.
- [88] An Efficient Heuristic for Defense Against Distributed Denial of Service Attacks using Route-Based Distributed Packet Filtering. Michael A. Schneider and Edward W. Felten. Submitted for publication, 2003.
- [89] Written testimony to House Commerce Committee, Subcommittee on Courts, the Internet, and Intellectual Property, oversight hearing on "Piracy of Intellectual Property on Peer to Peer Networks." September 2002.
- [90] Written testimony to Senate Judiciary Committee hearings on "Competition, Innovation, and Public Policy in the Digital Age: Is the Marketplace Working to Protect Digital Creativity?" March 2002.
- [91] Informed Consent Online: A Conceptual Model and Design Principles. Batya Friedman, Edward W. Felten, and Lynette I. Millett. Technical Report 2000-12-2, Dept. of Computer Science and Engineering, University of Washington, Dec. 2000.
- [92] Mechanisms for Secure Modular Programming in Java. Lujo Bauer, Andrew W. Appel, and Edward W. Felten. Technical Report CS-TR-603-99, Department of Computer Science, Princeton University, July 1999.
- [93] A Java Filter. Dirk Balfanz and Edward W. Felten. Technical Report 567-97, Dept. of Computer Science, Princeton University, October 1997.
- [94] Inside RISKS: Webware Security. Edward W. Felten. *Communications of the ACM*, 40(4):130, 1997.
- [95] Simplifying Distributed File Systems Using a Shared Logical Disk. Robert A. Shillner and Edward W. Felten. Princeton University technical report TR-524-96.

- [96] Contention and Queueing in an Experimental Multicomputer: Analytical and Simulation-based Results. Wenjia Fang, Edward W. Felten, and Margaret Martonosi. Princeton University technical report TR-508-96.
- [97] Design and Implementation of NX Message Passing Using SHRIMP Virtual Memory Mapped Communication. Richard D. Alpert, Cezary Dubnicki, Edward W. Felten, and Kai Li. Princeton University technical report TR-507-96.
- [98] Protocol Compilation: High-Performance Communication for Parallel Programs. Edward W. Felten. Ph.D. dissertation, Dept. of Computer Science and Engineering, University of Washington, August 1993.
- [99] Building Counting Networks from Larger Balancers. Edward W. Felten, Anthony LaMarca, and Richard Ladner. Univ. of Washington technical report UW-CSE-93-04-09.
- [100] The Case for Application-Specific Communication Protocols. Edward W. Felten. Univ. of Washington technical report TR-92-03-11.
- [101] A Centralized Token-Based Algorithm for Distributed Mutual Exclusion. Edward W. Felten and Michael Rabinovich. Univ. of Washington technical report TR-92-02-02.
- [102] Issues in the Implementation of a Remote Memory Paging System. Edward W. Felten and John Zahorjan. Univ. of Washington technical report TR-91-03-09.



## OFFICE OF SECRETARY OF STATE

*I, Karen C. Handel, Secretary of State of the State of Georgia, do  
hereby certify that*

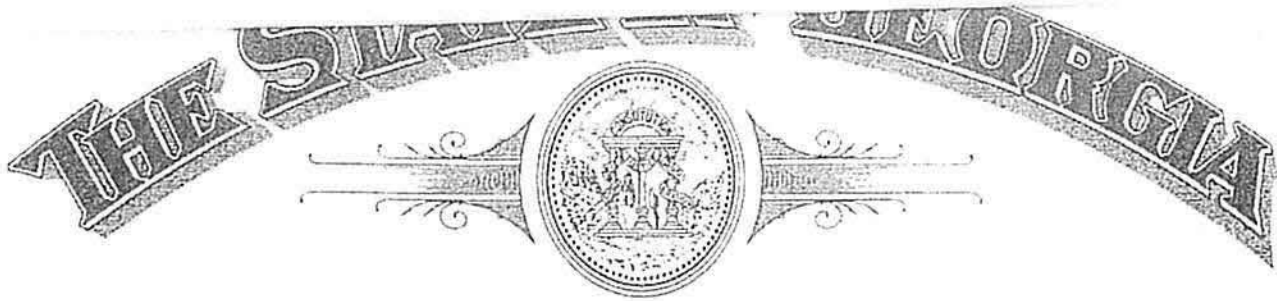
the attached nine pages, labeled A through I, are true and correct copies  
of voting equipment certifications; all as same appear on file in this office.

Plaintiff's Exhibit  
10  
06/07/2017 Hearing

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed  
the seal of my office, at the Capitol, in the City of Atlanta,  
this 18th day of April, in the year of our Lord Two  
Thousand and Eight and of the Independence of the United  
States of America the Two Hundred and Thirty-Second.



*Karen C. Handel*  
Karen C. Handel, Secretary of State



## OFFICE OF SECRETARY OF STATE

*I, Karen C. Handel, Secretary of State of the State of Georgia, do  
hereby certify that*

the attached one (1) page constitutes a true and correct copy of the certification of the AccuVote TS R6 Voting System, consisting of GEMS Version 1.1822G, AVTS firmware version 4.5.2, AVOS firmware version 1.94W, Encoder software 1.3.2, and Key Card Tools 1.0.1, manufactured by Diebold Election Systems, Inc., 1611 Wilmet Road, McKinney, Texas 75069, for use by the electors of the State of Georgia in all primaries and elections as provided in Georgia Election Code 21-2; all as same appear on file in this office.



IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 27th day of November, in the year of our Lord Two Thousand and Seven and of the Independence of the United States of America the Two Hundred and Thirty-Second.

*Karen C. Handel*

Karen C. Handel, Secretary of State



## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby  
certify that*

The AccuVote TS R6 and the AccuVote TSX Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 10th day of July, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirty-First.



*Cathy Cox*  
Cathy Cox, Secretary of State



## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby  
certify that*

For the purposes of a Conditional Interim Certification the AccuVote TS R6 and the AccuVote TSX Voting System, consisting of GEMS version 1.18.24, AVTS firmware version 4.6.4, and AVTS voting stations with the attached AccuView Printer Module (The following components of the Georgia voting system were included in the test to verify compatibility: GEMS 1.18.22G, AccuVote TS R6 voting stations with firmware AVTS 4.5.2, AccuVote TSX voting stations with AccuVote firmware AVTS 4.5.2, and ExpressPoll 4000 1.2.0.), manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; the Conditional Interim Certification shall expire on December 31, 2006.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 9th day of August, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirty-First.



*Cathy Cox*

Cathy Cox, Secretary of State



## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby  
certify that*

The AccuVote TS R6 and the AccuVote TSX Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1253 Allen Station Parkway, Allen, Texas 75002, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 14th day of April, in the year of our Lord Two Thousand and Six and of the Independence of the United States of America the Two Hundred and Thirtieth.



A handwritten signature of Cathy Cox in black ink, written over a horizontal line.

Cathy Cox, Secretary of State



## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby  
certify that*

The AccuVote TS R6 Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1611 Wilmeth Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 20th day of September, in the year of our Lord Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.



*Cathy Cox*  
Cathy Cox, Secretary of State



## OFFICE OF SECRETARY OF STATE

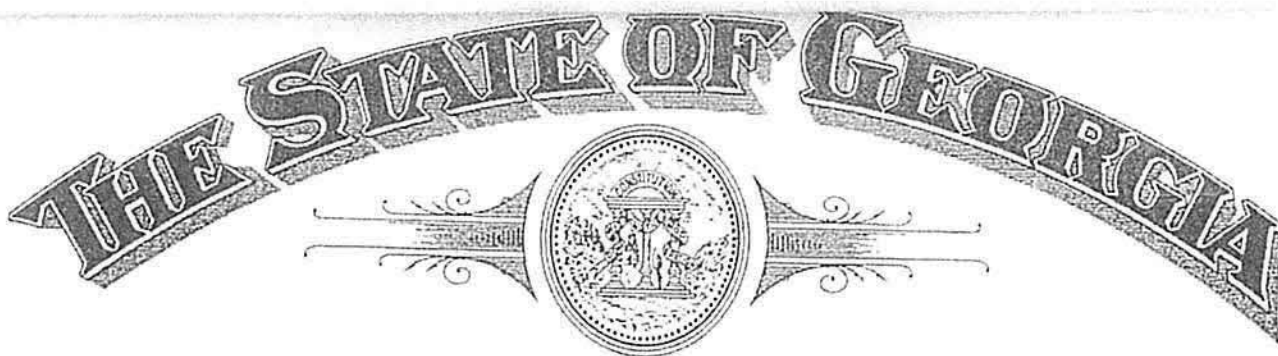
*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby  
certify that*

The AccuVote TS R6 Voting system, consisting of GEMS version 1.18.22G, AVTS firmware version 4.5.2, AVOS version 1.94w, Encoder software version 1.3.2, Key Card Tool 1.01, and ExpressPoll version 1.2.53, manufactured by Diebold Election Systems, Inc., 1611 Wilmet Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules and Regulations of the State Election Board, and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided however, I hereby reserve my opinion to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 20th day of September, in the year of our Lord Two Thousand and Five and of the Independence of the United States of America the Two Hundred and Thirtieth.



*Cathy Cox*  
Cathy Cox, Secretary of State



## OFFICE OF SECRETARY OF STATE

*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby  
certify that*

the AccuVote TS R6 Voting System, consisting of GEMS Version 1.18.22G, AVTS firmware version 4.5.2, AVOS firmware version 1.94W, Encoder software 1.3.2, and Key Card Tools 1.0.1, manufactured by Diebold Election Systems, Inc., 1611 Wilmet Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.



IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 31st day of December, in the year of our Lord Two Thousand and Four and of the Independence of the United States of America the Two Hundred and Twenty-Ninth.

A handwritten signature in cursive script, reading "Cathy Cox".

Cathy Cox, Secretary of State



*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that*

the AccuVote TS R6 Voting

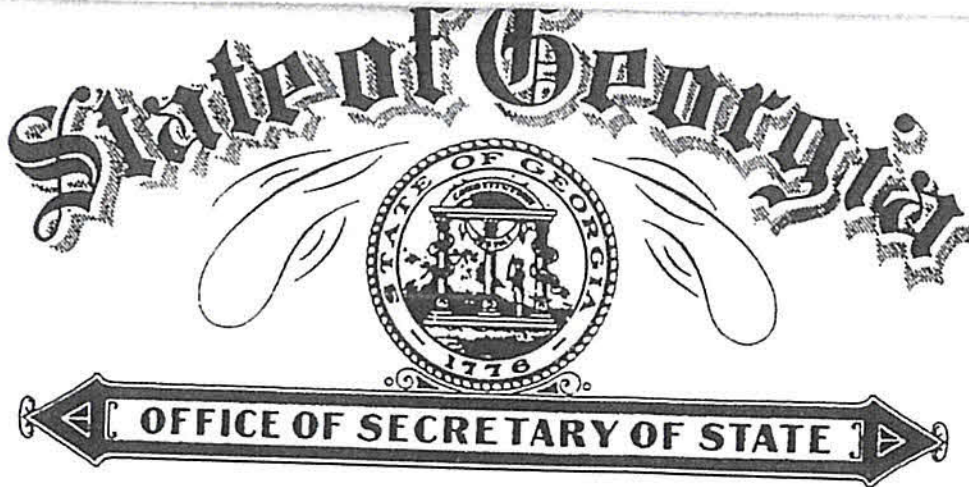
System, consisting of GEMS Version 1.18.15, and the AVTS firmware, Version 4.3.14, manufactured by Diebold Election Systems, Inc., 1611 Wilmet Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.

IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 10<sup>th</sup> day of February, in the year of our Lord Two Thousand and Three and of the Independence of the United States of America the Two Hundred and Twenty-ninth



*Cathy Cox*

SECRETARY OF STATE



*I, Cathy Cox, Secretary of State of the State of Georgia, do hereby certify that*

the AccuVote TS R6 Voting

System, consisting of the AVTS firmware, Version 4.1.11, manufactured by Diebold Election Systems, Inc., 1611 Wilmet Road, McKinney, Texas 75069, has been thoroughly examined and tested and found to be in compliance with the applicable provisions of the Georgia Election Code, the Rules of the State Elections Board and the Rules of the Secretary of State, and as a result of this inspection, it is my opinion that this kind of Direct Record Electronic voting system and its components can be safely used by the electors of this state in all primaries and elections as provided in Georgia Election Code 21-2; provided, however, I hereby reserve my option to reexamine this Direct Record Electronic voting system and its components at anytime so as to insure that it continues to be one that can be safely used by the voters of this state.



IN TESTIMONY WHEREOF, I have hereunto set my hand and affixed the seal of my office, at the Capitol, in the City of Atlanta, this 23<sup>th</sup> day of May, in the year of our Lord Two Thousand and Two and of the Independence of the United States of America the Two Hundred and Twenty-sixth

*Cathy Cox*

SECRETARY OF STATE

Schedule O (Form 990 or 990-EZ) 2014

Page 2

Name of the organization

Employer identification number

ROCKY MOUNTAIN FOUNDATION INC.

26-3670783

POLICY LITIGATION.

ATTACHMENT 1FORM 990, PART III, LINE 1 - ORGANIZATION'S MISSION

THE INTERESTS OF THE ROCKY MOUNTAIN FOUNDATION ARE CONSTITUTIONAL LIBERTIES AND THE INDIVIDUAL RIGHTS OF CITIZENS, WITH EMPHASIS ON FIRST AMENDMENT RIGHT, ELECTIONS, GOVERNMENT TRANSPARENCY AND ACCOUNTABILITY, OPEN RECORDS AND OPEN MEETINGS, DUE PROCESS, AND EQUAL PROTECTION OF THE LAWS. IT WILL ENGAGE IN LITIGATION AS WELL AS PROVIDE MONETARY SUPPORT FOR LEGAL EXPENSES TO OTHER ORGANIZATIONS ENGAGED IN LITIGATION ON THESE ISSUES. IT WILL ALSO INFORM LEGISLATIVE POLICY, PERFORM INDEPENDENT RESEARCH AND ANALYSIS IN THE FOREGOING SUBJECT AREAS. LASTLY, THE ORGANIZATION WILL USE GENERALLY AVAILABLE MEANS OF EDUCATION AND COMMUNICATION TO ILLUMINATE AND SHARE PUBLIC DEBATES ESPECIALLY AS ITS SUBJECTS OF INTEREST APPEAR TO BEAR UPON THE CITIZENS OF COLORADO AND THE REGION.

Plaintiff's Exhibit

14

06/07/2017 Hearing

JSA

Schedule O (Form 990 or 990-EZ) 2014

4E1228 1.000

9881HI 5974 10/29/2015 3:25:48 PM

1156879

Monday, June 5, 2017 at 11:55:11 AM Eastern Daylight Time

**Subject:** Re: FOIA request Georgia system certification

**Date:** Monday, June 5, 2017 at 10:23:11 AM Eastern Daylight Time

**From:** Marilyn Marks

**To:** Jeff Milsteen

Mr. Milsteen,  
Thank you for your reply.

To be clear, I am aware that Open Records requests should seek documentation, not pose interrogatories. My requests below are all composed to seek public records described, and not to pose questions to the officials. If you believe that some of the requests below are not probably styled as Open Records requests and instead reflect interrogatories, please let me know so that I may clarify. Feel free to call me, if you prefer to discuss. You may call me at 970 404 2225.

Thank you.  
Marilyn Marks

-----Original Message-----

**From:** Jeff Milsteen <jmilstee@kennesaw.edu>

**Date:** Monday, June 5, 2017 at 9:39 AM

**To:** Marilyn Marks <marilyn@aspenoffice.com>

**Subject:** Re: FOIA request Georgia system certification

Ms. Marks,

We are attempting to identify documentation that would be responsive to your additional open records requests. As you know, we are not compelled to respond to "interrogatories" or other questions -- our only obligation is to provide responsive documents. Please be assured we will do our best to identify and make that documentation available as soon as we are able to do so. We will not, however, be able to do that at 1:00 p.m. today. As soon as we have the documents available, I will let you know. Thanks.

Jeff

----- Original Message -----

**From:** "marilyn" <marilyn@aspenoffice.com>

**To:** "Jeff Milsteen" <jmilstee@kennesaw.edu>

**Sent:** Friday, June 2, 2017 4:16:35 PM

**Subject:** Re: FOIA request Georgia system certification

Mr. Milsteen,

I am attempting to clarify the responses to my FOIA request and better understand the nature of the state and federal certifications of the current voting system in Georgia.

In relation to the requests in the emails below, I seek documentation that of all system modifications made to the most recently state certified system were permitted by the provisions of SOS Certification Rule 590-8-1-.01(b)(4) below and approved by the Secretary of State:

Any modification to the hardware, firmware, or software of a



Page 1 of 12

voting system which has completed Qualification, Certification, or Acceptance testing in accordance with these Rules shall invalidate the State certification unless it can be shown that the modification does not affect the overall flow of program control or the manner in which the ballots are recorded and the vote data are processed, and the modification falls into one of the following classifications listed below. The Secretary of State shall be the sole judge of whether or not a modification requires additional testing.

(i) The modification is made for the purpose of correcting a defect and procedural and test documentation is provided which verifies that the installation of the hardware change or corrected code does not result in any consequence other than the elimination of the defect.

(ii) The modification is made for the purpose of enabling interaction with other general purpose or approved equipment or computer programs and databases, and procedural and test documentation is provided which verifies that such interaction does not involve or adversely affect vote counting and data storage.

5.

I seek documentation of the Secretary of State's decision as to whether all such modifications required testing.

I seek documentation of any and all defects as referenced in paragraph (i) for which a modification was made.

I seek documentation of any and all modifications in accordance with the provisions of paragraph (ii) and the test results documentation required for the modification.

I seek documentation for approving the inclusion of Easy Vote hardware and software in the Georgia voting system. I call your attention to 1990 VSS standard:

1.3.1 Voting Systems

A voting system is a combination of mechanical, electromechanical or electronic equipment-including the software and firmware required to program and to control the equipment-that is used to cast and count votes. Equipment that is not an integral part of a voting system, but that can be used as an adjunct to it, is considered to be a component of the system.

I would like to accept your offer to see the test results reports of all the currently used components. I do not seek any proprietary information and am satisfied to merely review the test summary conclusions signed by the testing agent. I would like to review these documents a 1pm on Monday, June 5 if that time is acceptable.

Merle King reportedly stated to the Atlanta Journal Constitution in September, 2016 that Georgia's system is federally certified. Please provide the federal certification supporting documentation for that statement.

The attached slides were presented by Mr. King. Note the statement on page 17 that the system is state certified. Please provide documentation supporting that claim.

The slide on page 17 states that the system is certified by NASED/FEC. Please provide documentation supporting that claim.

Thank you for your consideration. Feel free to contact me with any questions.

Marilyn Marks

Rocky Mountain Foundation

970 404 2225

-----Original Message-----

From: Marilyn Marks <[marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)>

Date: Friday, June 2, 2017 at 11:49 AM

To: Jeff Milsteen <jmilstee@kennesaw.edu>

Subject: Re: FOIA request Georgia system certification

Thank you, Mr. Milsteen.

I assume that CES/KSU maintains a copy of all state and federal certifications of Georgia voting systems. Is that correct?

In my original request of May 19 below, I requested correspondence between CES and federal voting systems certification organizations (NASED and EAC) for the current voting system. You responded that you had no documents responsive to that request. I assume that your office would be a custodian of any such documents and correspondence related to certification of Georgia voting systems. Is that correct? If CES is not the custodian, please inform me of the name of the custodian of such records.

Please send me a copy of the most recent state certification of Georgia's voting system, regardless of the system it certified.

Please send me a copy of the most recent federal certification of Georgia's voting system, regardless of the system it certified.

Thank you for your continued help.

Marilyn Marks

Executive Director

Rocky Mountain Foundation

-----Original Message-----

From: Jeff Milsteen <[jmilstee@kennesaw.edu](mailto:jmilstee@kennesaw.edu)>

Date: Friday, June 2, 2017 at 8:57 AM

To: Marilyn Marks <[marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)>

Subject: Re: FOIA request Georgia system certification

Ms. Marks,

Yes, my earlier response applied to both state and federal certification documents. Thanks.

Jeff

----- Original Message -----

From: "marilyn" <[marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)>

To: "Jeff Milsteen" <[jmilstee@kennesaw.edu](mailto:jmilstee@kennesaw.edu)>

Sent: Wednesday, May 31, 2017 5:37:29 PM

Subject: Re: FOIA request Georgia system certification

Mr. Milsteen,

Thank you for your response.

For clarification, does your response relate to both federal certification and state certification documents? If you possess a state certification for this system configuration listed below, please forward an electronic copy to my email.

Thank you.

Marilyn Marks

Rocky Mountain Foundation

-----Original Message-----

From: Jeff Milsteen <[jmilstee@kennesaw.edu](mailto:jmilstee@kennesaw.edu)>

Date: Wednesday, May 31, 2017 at 2:53 PM

To: Marilyn Marks <[marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)>

Subject: Re: FOIA request Georgia system certification

Ms. Marks,

I apologize for the delay in responding to your follow-up question regarding your open records request. I am advised that 1.1822G! is being used in the current elections. As for the date of certification, the CES has no documentation that would reflect that information.

Thanks.

Jeff

----- Original Message -----

From: "marilyn" <[marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)>

To: "Jeff Milsteen" <[jmilstee@kennesaw.edu](mailto:jmilstee@kennesaw.edu)>

Sent: Wednesday, May 24, 2017 1:04:22 PM

Subject: Re: FOIA request Georgia system certification

Thank you, Mr. Milsteen.

Please clarify whether 1.18.22G or 1.18.22G! is being used in current elections. I had asked about each of them in the FOIA request below.

Please provide the date of certification of 1.18. 22G and also for 1.18.22G!.

Thank you for your consideration.

Marilyn Marks

Rocky Mountain Foundation

From: Jeff Milsteen <[jmilstee@kennesaw.edu](mailto:jmilstee@kennesaw.edu)>

Date: Wednesday, May 24, 2017 at 10:56 AM

To: Marilyn Marks <[marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)>

Subject: Fwd: FOIA request Georgia system certification

This was inadvertently mis-addressed so I am resending.

Sent from my iPhone

Begin forwarded message:

From: Jeff Milsteen <[jmilstee@kennesaw.edu](mailto:jmilstee@kennesaw.edu)<<mailto:jmilstee@kennesaw.edu>>>

Date: May 24, 2017 at 9:45:58 AM EDT

To: [marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)<<mailto:marilyn@aspenoffice.com>>

Cc: [donnapr8@icloud.com](mailto:donnapr8@icloud.com)<<mailto:donnapr8@icloud.com>>

Subject: Fwd: FOIA request Georgia system certification

Ms. Marks:

This responds to your open records request, copied below, to Merle King, the Executive Director of the Center for Election Systems at Kennesaw State University. Should you have any questions about this response, please let me know.

With respect to your first request, the CES has no documents responsive to your request.

With respect to your second request, your email correctly identifies the components and related firmware and software used in Georgia, with the following addition: Honeywell barcode scanner MK1690-38-12-ISI, used in conjunction with the ExpressPoll electronic pollbooks.

With respect to your third request, we will make copies of certification documentation for all components of the voting system available for inspection at a mutually convenient date and time. However, these documents contain certain testing documents from ES&S that may contain trade secrets and be proprietary in nature and may require permission before they can be released. Please advise whether you wish to view these specific testing documents, in which case we will advise ES&S of your request.

With respect to requests number four and five, we have no documents responsive to your request.

Jeff Milsteen

Chief Legal Affairs Officer

Kennesaw State University

cc: Donna Price

From: "Donna Price Studio" <[donnapricestudio@gmail.com](mailto:donnapricestudio@gmail.com)<[<mailto:donnapricestudio@gmail.com>>](mailto:donnapricestudio@gmail.com)>

To: "Merle S. King" <[mking@kennesaw.edu](mailto:mking@kennesaw.edu)<[<mailto:mking@kennesaw.edu>>](mailto:mking@kennesaw.edu)>, "mbarne28" <[mbarne28@kennesaw.edu](mailto:mbarne28@kennesaw.edu)<[<mailto:mbarne28@kennesaw.edu>>](mailto:mbarne28@kennesaw.edu)>

Cc: "marilyn Marks" <[marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)<[<mailto:marilyn@aspenoffice.com>>](mailto:marilyn@aspenoffice.com)>

Sent: Sunday, May 21, 2017 7:14:31 PM

Subject: FOIA request Georgia system certification

Dear Mr. Merle King,

Under the Georgia Open Records Act § 50.18.70 et seq., I am writing add my name to the FOIA request of May 19, 2017 by Marilyn Marks of the Rocky Mountain Foundation, a copy of which is included in this email.

Should you have any questions, please do not hesitate to contact me at 404-354-2172 or via email at [donnapr8@icloud.com](mailto:donnapr8@icloud.com)<<mailto:donnapr8@icloud.com>> .

Thank you for your assistance.

Yours sincerely,

Donna Price

650 Pepperwood Lane

Stone Mountain, Georgia 30087

From: Marilyn Marks <[marilyn@aspenoffice.com](mailto:marilyn@aspenoffice.com)<<mailto:marilyn@aspenoffice.com>> >

Date: Friday, May 19, 2017 at 1:48 PM

To: " [mking@kennesaw.edu](mailto:mking@kennesaw.edu)<<mailto:mking@kennesaw.edu>> " <[mking@kennesaw.edu](mailto:mking@kennesaw.edu)<<mailto:mking@kennesaw.edu>> >

Cc: " [mbarne28@kennesaw.edu](mailto:mbarne28@kennesaw.edu)<<mailto:mbarne28@kennesaw.edu>> " <[mbarne28@kennesaw.edu](mailto:mbarne28@kennesaw.edu)<<mailto:mbarne28@kennesaw.edu>> >, Duncan Buell <[buell@acm.org](mailto:buell@acm.org)<<mailto:buell@acm.org>> >

Subject: FOIA request Georgia system certification

Mr. King:

Under the Georgia Open Records Act § 50.18.70 et seq., Rocky Mountain Foundation is requesting electronic copies of the following public records related to current Georgia voting systems. We understand the system in use to include:

Optical Scan

AccuVote OS 1.94W

Touch Screen

R6 – Ballot Station 4.5.2!

TSx – Ballot Station 4.5.2!

ExpressPoll

Express Poll 2.1.2

Security Key 4.5

Election Management System

GEMS 1.18.22 G

The source of our information is Georgia's Logic and Accuracy Testing Manual v1.4

( [https://www.eac.gov/assets/1/28/Logic\\_and\\_Accuracy\\_Testing\\_Manual\\_Final\\_v1.4.pdf](https://www.eac.gov/assets/1/28/Logic_and_Accuracy_Testing_Manual_Final_v1.4.pdf) )

Additionally, GEMS 1.18.22G! was referenced by CES as in use in Georgia. ( <http://grouper.ieee.org/groups/1622/WorkingDocuments/meeting-2014-02-GTRI/AllSlides-v12.pdf> )

We do not find this GEMS system configuration listed in NASED certified systems. ( <https://www.nased.org/NASED%20Qualified%20Voting%20Systems%20FINAL%20rev081407.pdf> )

1. Please provide a copy of the statement of NASED or other federal standard certification that covers the current Georgia voting system in its present configuration, similar to the information provided for other systems' certified and documented in NASED link above.

2. Please provide a copy of the list of components and related firmware and software versions in use.

3. Please provide a copy of certification documentation supporting the certification claims in the attached

slide, for use of the system in its current configuration, including the use of TSx machines as intermediary transmission devices for votes cast on TS machines.

4. Please provide the latest correspondence between your organization and NASED and/or EAC regarding or related to certification of Georgia's current voting system.

5. Please provide a copy of the system definition document required by 1990 VSS section B.2.3.1 .

If there are any fees for searching or copying these records, please inform me if the cost will exceed \$100. However, Rocky Mountain Foundation, a non-partisan 501(c) (3) organization, with members who are residents of Georgia, requests a waiver of all fees because the disclosure of the requested information is in the public interest and will contribute significantly to the public's understanding of the operations of electronic voting equipment and reporting of results. This information is not being sought for commercial purposes.

The Georgia Open Records Act requires a response time within three business days. If access to the records I am requesting will take longer than three days, please contact me with information about when I might expect copies or the ability to inspect the requested records.

If you deny any or all of this request, please cite each specific exemption on which you base your denial of the election information and notify me of the appeal procedures available to me under the law. Thank you for your consideration. Please contact me at the email or phone number below with any questions.

Sincerely,

Marilyn Marks

Exec. Director Rocky Mountain Foundation

7035 Marching Duck Drive E504 Charlotte, NC 28210

704-552-1618

[Marilyn@RockyMountainFoundation.org](mailto:Marilyn@RockyMountainFoundation.org)<<mailto:Marilyn@RockyMountainFoundation.org>>

--

Merle S. King

Executive Director

Center for Election Systems

Kennesaw State University

3205 Campus Loop Road

Kennesaw, Georgia 30144

Voice: 470-578-6900

Fax: 470-578-9012

Rocky Mountain Foundation, Inc. has one or more members in each of the counties--  
DeKalb, Fulton and Cobb - who are Sixth Congressional District voters.

Fulton:

Donna Curling  
11200 Bowen Road  
Roswell, GA 30075

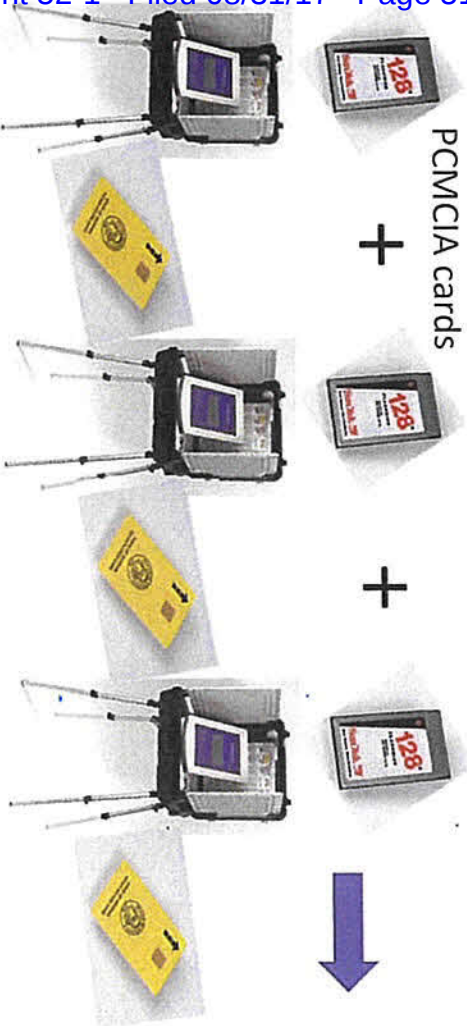
Cobb:

Michael Opitz  
1802 Wynfair Court,  
Marietta, GA 30062

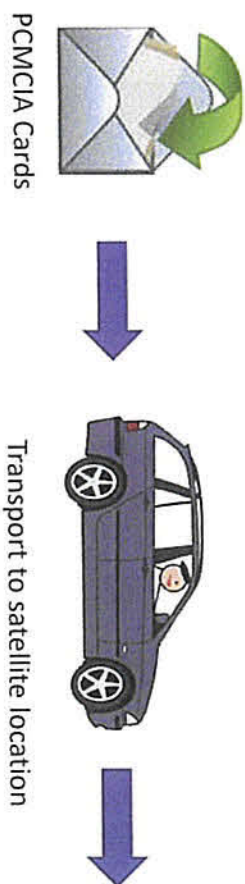
DeKalb:

XUAN HOA NGUYEN  
3379 Spring Harbor Dr.  
Doraville, Ga. 30340

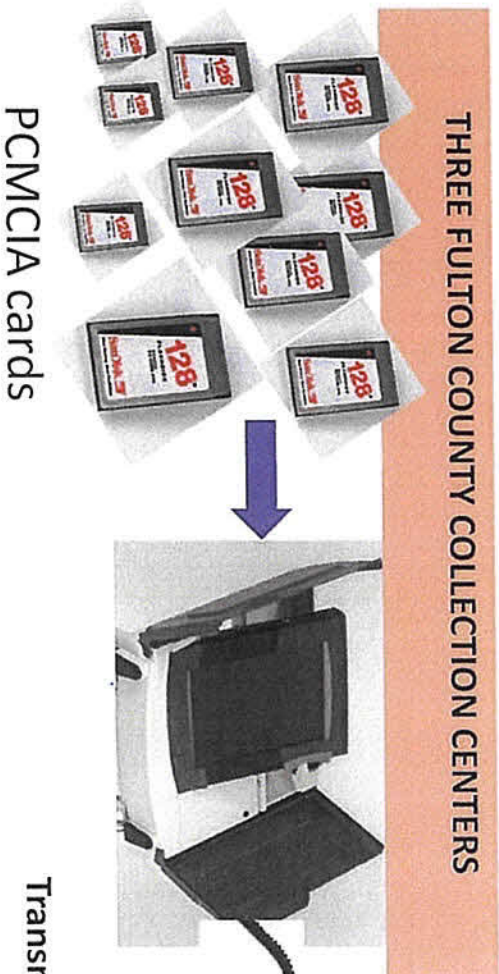
IN EACH PRECINCT:



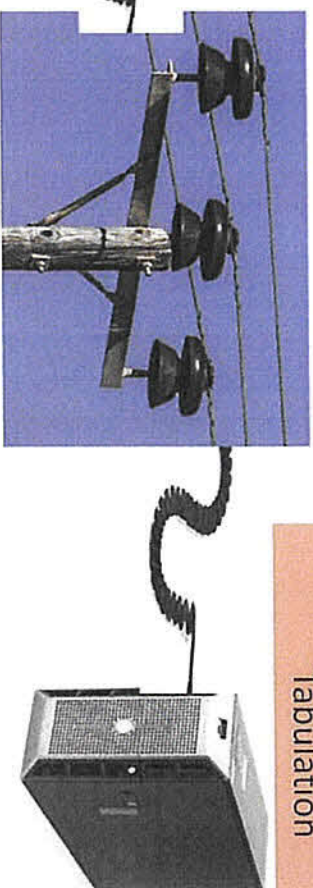
## Fulton County Election Data Flow



THREE FULTON COUNTY COLLECTION CENTERS



GEMS Central Server  
Tabulation



# COMPONENTS IN USE ARE NOT CERTIFIED AS A SYSTEM

COMPONENTS	SYSTEM COMPONENTS IN USE PER KSU OPEN RECORDS RESPONSE 6/1/2017	SEC. OF STATE VOTING SYSTEM CERTIFICATION 11/27/2007	STATE CERTIFICATION FOR TSx COMPONENT 05/14/2015
Election Management System	1.18.22G!	1.18.22G	
Touchscreen Machines:			
R6	4.5.2!	4.5.2	
TSx	4.5.2!	None	4.5.2!
Electronic Pollbook:			
Express Poll 4000	Express Pollbook 4000 Version Unknown	1.2.53	
Express Poll 5000	Exp 5000 Version 2.1.2	None	
Key Card Tool	4.5	1.01	
Paper Ballot Optical Scan:			
Accuvote OS	1.94W	1.94W	
Voter Card Encoder:			
Windows			
EasyVote – Voter Identification	In Use	None	



Colorado Secretary of State  
Date and Time: 11/04/2008 06:47 PM  
ID Number: 20081585735

Document must be filed electronically.  
Paper documents will not be accepted.

Document processing fee  
Fees & forms/cover sheets  
are subject to change.

\$50.00

Document number: 20081585735  
Amount Paid: \$50.00

To access other information or print  
copies of filed documents,  
visit [www.sos.state.co.us](http://www.sos.state.co.us) and  
select Business Center.

ABOVE SPACE FOR OFFICE USE ONLY

### Articles of Incorporation for a Nonprofit Corporation

filed pursuant to § 7-122-101 and § 7-122-102 of the Colorado Revised Statutes (C.R.S.)

1. The domestic entity name for the nonprofit corporation is

Rocky Mountain Foundation, Inc.

*(Caution: The use of certain terms or abbreviations are restricted by law. Read instructions for more information.)*

2. The principal office address of the nonprofit corporation's initial principal office is

Street address 3840 S. Willow Way  
(Street number and name)  
Denver CO 80237  
(City) (State) (ZIP/Postal Code)  
United States  
(Province – if applicable) (Country)

Mailing address  
(leave blank if same as street address) (Street number and name or Post Office Box information)  
(City) (State) (ZIP/Postal Code)  
(Province – if applicable) (Country)

3. The registered agent name and registered agent address of the nonprofit corporation's initial registered agent are

Name  
(if an individual) (Last) (First) (Middle) (Suffix)

OR

(if an entity) The Tipton Law Firm, P.C.  
(Caution: Do not provide both an individual and an entity name.)

Street address 3840 S. Willow Way  
(Street number and name)  
Denver CO 80237  
(City) (State) (ZIP Code)

**Mailing address**

(leave blank if same as street address)

(Street number and name or Post Office Box information)

(City)

CO  
(State)

(ZIP Code)

(The following statement is adopted by marking the box.)

- ☒ The person appointed as registered agent above has consented to being so appointed.

## 4. The true name and mailing address of the incorporator are

Name

(if an individual)

(Last)

(First)

(Middle)

(Suffix)

**OR**

(if an entity)

The Tipton Law Firm, P.C.

(Caution: Do not provide both an individual and an entity name.)

Mailing address

3840 S. Willow Way

(Street number and name or Post Office Box information)

Denver

(City)

CO

(State)

80237

(ZIP/Postal Code)

United States

(Province – if applicable)

(Country)

(If the following statement applies, adopt the statement by marking the box and include an attachment.)

- ☐ The corporation has one or more additional incorporators and the name and mailing address of each additional incorporator are stated in an attachment.

## 5. (If the following statement applies, adopt the statement by marking the box.)

- ☐ The nonprofit corporation will have voting members.

## 6. (The following statement is adopted by marking the box.)

- ☒ Provisions regarding the distribution of assets on dissolution are included in an attachment.

## 7. (If the following statement applies, adopt the statement by marking the box and include an attachment.)

- ☒ This document contains additional information as provided by law.

## 8. (Caution: Leave blank if the document does not have a delayed effective date. Stating a delayed effective date has significant legal consequences. Read instructions before entering a date.)

(If the following statement applies, adopt the statement by entering a date and, if applicable, time using the required format.)

The delayed effective date and, if applicable, time of this document is/are \_\_\_\_\_  
(mm/dd/yyyy hour:minute am/pm)

**Notice:**

Causing this document to be delivered to the Secretary of State for filing shall constitute the affirmation or acknowledgment of each individual causing such delivery, under penalties of perjury, that the document is the individual's act and deed, or that the individual in good faith believes the document is the act and deed of the person on whose behalf the individual is causing the document to be delivered for filing, taken in conformity with the requirements of part 3 of article 90 of title 7, C.R.S., the constituent documents, and the organic statutes, and that the individual in good faith believes the facts stated in the document are true and the document complies with the requirements of that Part, the constituent documents, and the organic statutes.

This perjury notice applies to each individual who causes this document to be delivered to the Secretary of State, whether or not such individual is named in the document as one who has caused it to be delivered.

9. The true name and mailing address of the individual causing the document to be delivered for filing are

Tipton	Cory		
<small>(Last)</small>	<small>(First)</small>	<small>(Middle)</small>	<small>(Suffix)</small>
3840 S. Willow Way			
<small>(Street number and name or Post Office Box information)</small>			
<hr/>			
Denver	CO	80237	
<small>(City)</small>	<small>(State)</small>	<small>(ZIP/Postal Code)</small>	
United States			
<small>(Province – if applicable)</small>	<small>(Country)</small>		

*(If the following statement applies, adopt the statement by marking the box and include an attachment.)*

- ☐ This document contains the true name and mailing address of one or more additional individuals causing the document to be delivered for filing.

**Disclaimer:**

This form/cover sheet, and any related instructions, are not intended to provide legal, business or tax advice, and are furnished without representation or warranty. While this form/cover sheet is believed to satisfy minimum legal requirements as of its revision date, compliance with applicable law, as the same may be amended from time to time, remains the responsibility of the user of this form/cover sheet. Questions should be addressed to the user's legal, business or tax advisor(s).

**Rocky Mountain Foundation, Inc.**  
**Attachment to**  
**Articles of Incorporation for the Nonprofit Corporation**

Provision 1: **Purpose.** Said corporation is organized exclusively for charitable, religious, educational, and scientific purposes, including, for such purposes, the making of distributions to organizations that qualify as exempt organizations under section 501(c)(3) of the Internal Revenue Code, or the corresponding section of any future federal tax code.

Provision 2: **Net Earnings.** No part of the net earnings of the corporation shall inure to the benefit of, or be distributable to its members, trustees, officers, or other private persons, except that the corporation shall be authorized and empowered to pay reasonable compensation for services rendered and to make payments and distributions in furtherance of the purposes set forth in Provision 1 hereof. No substantial part of the activities of the corporation shall be the carrying on of propaganda, or otherwise attempting to influence legislation, and the corporation shall not participate in, or intervene in (including the publishing or distribution of statements) any political campaign on behalf of or in opposition to any candidate for public office. Notwithstanding any other provision of these articles, this corporation shall not, except to an insubstantial degree, engage in any activities or exercise any powers that are not in furtherance of the purposes of this corporation.

Provision 3: **Distribution on Dissolution.** Upon the dissolution of the corporation, assets shall be distributed for one or more exempt purposes within the meaning of section 501(c)(3) of the Internal Revenue Code, or the corresponding section of any future federal tax code, or shall be distributed to the federal government, or to a state or local government, for a public purpose. Any such assets not so disposed of shall be disposed of by a Court of Competent Jurisdiction of the county in which the principal office of the corporation is then located, exclusively for such purposes or to such organization or organizations, as said Court shall determine, which are organized and operated exclusively for such purposes.

**CURLING000004**

C-E-R-T-I-F-I-C-A-T-E

STATE OF GEORGIA:

COUNTY OF FULTON:

I hereby certify that the foregoing transcript was taken down, as stated in the caption, and the colloquies, questions and answers were reduced to typewriting under my direction; that the foregoing pages represent a true and correct record of the evidence given.

I further certify that in accordance with OCGA 9-11-28(a) I am not a relative, employee, attorney, or counsel of any party, nor am I financially interested in the action.

This the 26th day of June 2017.

/s/ *Kristina Weaver*  
KRISTINA WEAVER, RPR, CCR-B-1785